

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

Effektivität und Wettbewerbsfähigkeit für Finanzdienstleister mit PSD2

[Nuance Communications](#)

14 Januar 2020



Finanztransaktionen und Kundeninteraktionen zählen zu den am häufigsten von Betrug betroffenen Prozessen. Um hier für mehr Sicherheit zu sorgen, wurde in der EU die Payment Services Directive 2 (PSD2) eingeführt. Mit ihrer Hilfe sollen Kunden künftig eindeutig verifiziert werden.

In Onlinehandel und -banking war der Begriff PSD2 sicherlich eines der Schlagworte des Jahres 2019. Dabei geht es um die am 14. September 2019 in Kraft getretene Richtlinie für Zahlungsdienstleistungen in Europa. Diese Regelung wurde von der EU umgesetzt, um den Zahlungsverkehr transparenter und sicherer zu gestalten. Für Betreiber von Onlineangeboten hat sie eine ganze Reihe von Folgen. So wachsen insbesondere im Bereich Authentifizierung in puncto Sicherheit die technischen und administrativen Anforderungen.

Bereits im Januar 2018 war eine erste Stufe der PSD2 umgesetzt worden. Damit sollen Zahlungsdienste in Europa modernisiert und betrugssicher gemacht werden. Die nun eingeführte zweite Stufe setzt auf den Einsatz wirksamer Methoden zur Kundenauthentifizierung. Dies betrifft nicht nur Banken, sondern alle Unternehmen, die online Finanzdienstleistungen und -transfers abwickeln. Damit stehen auch unzählige Onlinehändler vor der Aufgabe, ihre Authentifizierungsmodalitäten zu erneuern.

Die Auswirkungen von PSD2

PSD2 baut zwar auf dem derzeitigen Stand auf, doch wird es ein wichtiger Katalysator für die Revolution des Zahlungsverkehrs sein. „Open Banking“ wird endlich Wirklichkeit. Neue Anbieter können den Markt betreten und für die etablierten Finanzdienstleistungen ernstzunehmende Konkurrenz werden.

Der Verbraucherschutz wird durch mehr Kostentransparenz und Schutz vor zusätzlichen Gebühren gestärkt. Er wird auch von der erweiterten geografischen Reichweite der PSD2 und entsprechender

Beschränkung derzeitiger Ausnahmen profitieren. Damit soll Online-Betrug eingedämmt werden.

Die Sicherheitsrisiken im Zusammenhang mit dem elektronischen Zahlungsverkehr sind in den letzten Jahren gestiegen. Dies ist zum Teil auch auf die zunehmende technische Komplexität, das stetig wachsende Aufkommen elektronischer Zahlungen sowie auf die Entwicklung neuer Zahlungsarten zurückzuführen. Finanzdienstleister müssen hier neue Wege der Dokumentation über die Einhaltung der Vorgaben beschreiten.

Mehr Sicherheit für Kunden

Zu den wichtigsten Neuerungen gehören dabei neue Vorschriften zur Identifikation und Verifikation von Kunden. Ein Bestandteil ist die Schaffung einer Strong Customer Authentication (SCA). Dabei geht es um Standards, mit denen die Sicherheit der Kunden und ihrer Daten gewährleistet werden soll. Das Einsatzgebiet umfasst Online-Finanztransaktionen, aber auch die Nutzung kanalübergreifender, biometrischer Zugangsmethoden.

Um Sicherheit zu gewährleisten, schreibt die PSD2 eine Zwei-Faktor-Authentifizierung vor. Dieses Prinzip wird beim Onlinebanking deutlich, wo sich Kunden bereits bei der Anmeldung zweifach identifizieren müssen, um Zugriff auf ihre Kontodaten zu erhalten. Gleiches gilt beim Onlineshopping: Dort müssen Händler für ihre Kunden beim Checkout eine zusätzliche Authentifizierung in den Prozess integrieren. Dabei müssen mindestens zwei der folgenden drei Merkmale verwendet werden:

- Wissen: Ein Merkmal, das nur der Nutzer kennt (z. B. PIN, Passwort)
- Besitz: Ein Merkmal, das nur der Nutzer besitzt (z. B. mobile TAN)
- Inhärenz: Ein Merkmal, das nur dem Nutzer eigen ist (z. B. biometrische Eigenschaften)

Um die geforderte Sicherheit zu gewährleisten, dürfen diese drei Eigenschaften nicht miteinander zusammenhängen oder interagieren.

PSD2 erfolgreich und datenschutzkonform implementieren

Die Erstellung reibungslos laufender Prozesse unter Berücksichtigung dieser Maßgaben ist äußerst komplex. Finanzdienstleister benötigen hierfür Lösungen, die wenigstens zwei der drei erforderlichen Identifizierungsmethoden bieten. Die von Nuance bereitgestellten innovativen biometrischen und nicht-biometrischen Technologien bieten zum Beispiel :

- Eine äußerst sichere inhärente Verifizierung ist durch den Einsatz von **Sprachbiometrie** gegeben. Diese Methode ist für Kunden gleichzeitig äußerst bequem, da sie sich keine umständlichen Passwörter oder PINs merken müssen.
- Der **Device Print** erstellt einen nicht-biometrischen „Abdruck“ basierend auf dem Gerät, das bei der Registrierung verwendet wurde. Damit kann das Gerät während neuer Kundenanfragen überprüft und zur weiteren Interaktion freigegeben werden..

Ausgefeilte Controlling-Funktionen

Bei all der Verifizierungstechnologie darf die Analyse der Daten nicht zu kurz kommen. Lösungen wie Nuance Analytics geben automatisch aussagekräftige Einblicke und Hintergrunddaten zu Omni-Channel-Kundeninteraktionen. Damit sind Unternehmen über die Performance bei Anrufen, Live-Chats, SMS, E-Mails oder Social Media-Posts stets bestens informiert.

Neben Sicherheit und Leistungsübersichten spielt auch die Schnelligkeit eine wichtige Rolle. Finanzdienstleister sollten darauf achten, ein System auszusuchen, das sich schnell in bereits bestehende Umgebungen einbinden lässt. Die Nuance-Lösungen für Analysen der Kundeninteraktion sind blitzschnell einsatzbereit: Mit den leistungsstarken APIs wird die individuelle Anpassung vereinfacht, damit das System direkt und unkompliziert eingesetzt werden kann. Darüber hinaus optimiert Nuance Analytics durch die automatisierte Überwachung von Agenten-Performance, Scoring, Alarmierung und Anrufintervention die Qualitätssicherung sowie die Einhaltung der Compliance-Richtlinien im Unternehmen.

Authentifizierungstechnologien von Nuance unterstützen Unternehmen bei diesem Vorhaben. Ihr Ziel ist dabei die Schaffung eines ebenso sicheren wie bequemen Kundenerlebnisses.

Tags: [Sprachbiometrie](#), [Spracherkennung](#), [Sprachtechnologie](#), [Biometrische Authentifizierung](#)